IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Before the Board of Patent Appeals and Interferences

Application No.	:	10/549,465
Appellants	:	Junbiao Zhang and Saurabh Mathur
Filed	:	14 September 2005
For	:	A FLEXIBLE WLAN ACCESS POINT ARCHITECTURE CAPABLE OF ACCOMMODATING DIFFERENT USER DEVICES
Art Unit	:	2431
Examiner	:	Syed Zia
Conf. No.	:	8383

Appeal Brief

Commissioner for Patents
MAIL STOP APPEAL BRIEF - PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This is a Brief on appeal from the decision of the Examiner dated 10 November 2010, finally rejecting Claims 1-27, all of the Claims in the Application.

The Appellants request that the fee for this Brief be charged against Deposit Account No. 07-0832

Table of Contents

Real Party in Interest

The real party in interest is:

THOMSON LICENSING S.A.,
46 Quai A. LeGallo
F-92100 Boulogne Billancourt
France,

the assignee of the entire right, title and interest in and to the subject application, by virtue of an assignment recorded with the US Patent and Trademark Office on 8 November 2005, at Reel/Frame 016985/0270.

Related Appeals and Interferences

The Appellants assert that no other appeals or interferences are known to the Appellants, the Appellants' legal representatives or Assignee, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status of Claims

Claims 1-27 are pending. All of the pending Claims have been rejected. The rejection of Claims 1-27 is appealed.

Status of Amendments

All submitted amendments have been entered.

Summary of Claimed Subject Matter

The following sets forth independent Claims 1, 4, 10, 14 and 21, with parenthesized references to the instant Application as filed:

1. A method for controlling access by a user terminal to a communications network comprising the steps of:

receiving from the user terminal a request to access the communications network (page 9, line 5);

transmitting to the user terminal an identity request message (page 9, line 6);

receiving from the user terminal a response to the identity request message (page 9, lines 7-8);

determining whether the user terminal uses a predetermined authentication protocol in response to the response to the identity request message (page 9, lines 9-10);

selecting said predetermined authentication protocol if the user terminal uses said predetermined authentication protocol (page 3, lines 22-25); and

selecting an authentication mechanism compatible with the user terminal upon determining the user terminal is not compatible with the predetermined authentication protocol, for allowing user terminal access to the communications network (page 3, lines 18-20).

4. A method for controlling user terminal access to a wireless local area network, comprising the steps of:

receiving from a user terminal a request to access the wireless local area network (page 9, line 23);

transmitting to the user terminal an identity request message (page 9, line 24);

receiving from the user terminal a response to the identity request message (page 9, lines 25-26);

determining whether the user terminal is IEEE 802.1x compliant in response to the response to the identity request message (page 9, lines 27-28);

selecting an authenticating mechanism utilizing IEEE 802.1x if said user terminal is IEEE 802.1 x compliant (page 3, lines 22-25); and

selecting an authentication mechanism, compatible with the user terminal, in response to a determination that the user terminal is not IEEE 802.1x compliant, for allowing user terminal access to the wireless local area network (page 3, lines 18-20).

10. An access point in communication with a user terminal in a wireless local area network, comprising:

means to determine if the user terminal utilizes an IEEE 802.1x protocol (item 415; page 8, lines 8-10);

means for employing the IEEE 802.1 x. protocol in said access point, if said user terminal utilizes the IEEE 802.1x. protocol (page 8, lines 12-13); and,

means for employing an authentication means compatible with the user terminal if the user terminal employs a protocol other than the IEEE 802.1x protocol (page 8, lines 10-12).

14. A method for controlling access by a user terminal in a wireless local area network by determining whether the user terminal utilizes an IEEE 802.1x protocol comprising the steps of:

an access point communicating to the user terminal a request to identify, and if the user terminal utilizes an IEEE 802.1x protocol, acknowledging the request to identify, otherwise the access point determining that the user terminal is not IEEE 802.1x compliant and selecting an authentication mechanism compatible with the user terminal (page 11, lines 7-13).

21. A method for controlling access of a user terminal in a wireless local area network by determining whether the user terminal utilizes an IEEE 802.1x protocol, comprising the steps of:

communicating through an access point to the user terminal a request to identify, and if the user terminal utilizes an IEEE 802.1x protocol, acknowledging the request to identify, otherwise determining by the access point that the user terminal is not IEEE 802.1x compliant and selecting an authentication mechanism

compatible with the user terminal (page 12, lines 6-11).

Grounds of Rejection to be Reviewed On Appeal

a) Whether Claims 1, 4, 10, 14 and 21 have been properly rejected for failure to comply with 35 USC 112, as being indefinite.

b) Whether Claims 1-27 have been properly rejected for failure to comply with 35 USC 102(e), as being anticipated by US 7,483,984 to Jonker et al.

Remarks/Arguments

This invention relates to a method and access point for controlling access by a user terminal to a communications network, in which an authentication mechanism which is compatible with the user terminal is selected if the user terminal is not compatible with a predetermined authentication protocol. Nowhere is the claimed invention shown or suggested by the cited prior art.

a) The Examiner has rejected Claims 1, 4, 10, 14, and 21, under 35 USC 112 as not being clear as to how the recited selection mechanism is implemented. The implementation of the recited selection mechanism is explained in the instant specification from page 6, line 21, to page 7, line 15. The Appellants submit that 35 USC 112 does not require such explanation to be recited in independent claims. The Appellants therefore submit that the rejection of Claims 1, 4, 10, 14, and 21, under 35 USC 112, is clearly improper and should be reversed.

b) The Examiner has rejected Claims 1-27, all of the claims in the application, as anticipated, under 35 USC 102(e), by US 7,483,984 to Jonker et al.

Jonker et al relates to an arrangement which allows a client device to access a plurality of carrier networks. Jonker et al arrange a plurality of databases 116, 117, 118 and 120 as part of mobile computing device 102, so that mobile computing device 102 may have access to multiple carrier networks having different logon protocols. See column 4, line 33, to column 5, line 17, of Jonker et al. Such an arrangement requires each access client 100 and mobile computing device 102 to have separate databases. The instant invention solves this problem by associating such information with a network, so that the information does not have to be duplicated in each mobile computing device. Nowhere do Jonker et al show or suggest:

"selecting an authentication mechanism compatible with the user terminal upon determining the user terminal is not compatible with the predetermined authentication protocol, for allowing user terminal access to the communications network",

as specifically recited in Claim 1. Rather, Jonker et al disclose that each mobile device determines the wireless protocol of the network which is being accessed, and adjusts its protocol to match the protocol of the network. See column 5, line 56 to column 6, line 8. It is therefore clear that Jonker et al do not affect the patentability of Claim 1.

Claims 2 and 3 are dependent from Claim 1 and add further advantageous features. The Appellants submit that these subclaims are patentable as their parent Claim 1.

Similarly, nowhere do Jonker et al show or suggest:

"selecting an authentication mechanism, compatible with the user terminal, in response to a determination that the user terminal is not IEEE 802.1x compliant, for allowing user terminal access to the wireless local area network",

as specifically recited in Claim 4. It is therefore clear that Jonker et al do not affect the patentability of Claim 4.

Claims 5 to 9 are dependent from Claim 4 and add further advantageous features. The Appellants submit that these subclaims are patentable as their parent Claim 4.

Similarly, nowhere do Jonker et al show or suggest:

"means for employing an authentication means compatible with the user terminal if the user terminal employs a protocol other than the IEEE 802.1x protocol",

as specifically recited in Claim 10. It is therefore clear that Jonker et al do not affect the patentability of Claim 10.

Claims 11-13 are dependent from Claim 10 and add further advantageous features. The Applicants submit that these subclaims are patentable as their parent Claim 10.

Similarly, nowhere do Jonker et al show or suggest:

"the access point determining that the user terminal is not IEEE802.1x compliant and selecting an authentication mechanism compatible with the user terminal",

as specifically recited in Claim 14. It is therefore clear that Jonker et al do not affect the patentability of Claim 14.

Claims 15-20 are dependent from Claim 14 and add further advantageous features. The Appellants submit that these subclaims are patentable as their parent Claim 14.

Similarly, nowhere do Jonker et al show or suggest:

"determining by the access point that the user terminal is not IEEE 802.1x compliant and selecting an authentication mechanism compatible with the user terminal",

as specifically recited in Claim 21. It is therefore clear that Jonker et al do not affect the patentability of Claim 21.

Claims 22-27 are dependent from Claim 21 and add further advantageous features. The Appellants submit that these subclaims are patentable as their parent Claim 21.

The Appellants therefore submit that the final rejection is improper and should be reversed.

Respectfully submitted,
Junbiao Zhang
Saurabh Mathur

/Catherine A. Cooper/
by Catherine A. Cooper
Attorney for Applicant
Registration No. 40,877
609/734-6440

THOMSON Licensing LLC
Patent Operation
PO Box 5312
Princeton, NJ 08543-5312

Date: _7_March 2011

Claims Appendix

1. A method for controlling access by a user terminal to a communications network comprising the steps of:

receiving from the user terminal a request to access the communications network;

transmitting to the user terminal an identity request message;

receiving from the user terminal a response to the identity request message;

determining whether the user terminal uses a predetermined authentication protocol in response to the response to the identity request message;

selecting said predetermined authentication protocol if the user terminal uses said predetermined authentication protocol; and

selecting an authentication mechanism compatible with the user terminal upon determining the user terminal is not compatible with the predetermined authentication protocol, for allowing user terminal access to the communications network.

2. The method according to claim 1, wherein the communications network comprises a wireless local area network that complies with IEEE 802.11 standards.

3. The method according to claim 2, including selecting an appropriate authentication server coupled to the wireless local area network in response to the determination.

4. A method for controlling user terminal access to a wireless local area network, comprising the steps of:

receiving from a user terminal a request to access the wireless local area network;

transmitting to the user terminal an identity request message;

receiving from the user terminal a response to the identity request message;

determining whether the user terminal is IEEE 802.1x compliant in response to the response to the identity request message;

selecting an authenticating mechanism utilizing IEEE 802.1x if said user terminal is IEEE 802.1 x compliant; and

selecting an authentication mechanism, compatible with the user terminal, in response to a determination that the user terminal is not IEEE 802.1x compliant, for allowing user terminal access to the wireless local area network.

5. The method according to claim 4, further comprising the steps of, if the user terminal is IEEE 802.1x compliant, transmitting an authentication request to an authentication server and receiving an authentication response utilizing IEEE 802.1x protocol, and controlling user terminal access to the wireless local area network in response to the authentication response.

6. The method according to claim 4, further comprising the steps of, if the user terminal is not IEEE 802.1x compliant, redirecting an authentication request to an HTTP server for utilizing a browser based authentication protocol.

7. The method according to claim 6, further comprising the step of configuring a packet filtering module to redirect the authentication request to the HTTP server.

8. The method according to claim 7, further comprising the step of maintaining state information in the wireless local area network for use by the packet filtering module and the HTTP server.

9. The method according to claim 8, wherein the state information includes one of a first state indicative of ongoing authentication process, a second state indicative of authentication failure, a third state indicative of authentication success, and a fourth state indicative of a IEEE 802.1x noncompliant user terminal.

10. An access point in communication with a user terminal in a wireless local area network, comprising:

means to determine if the user terminal utilizes an IEEE 802.1x protocol;

means for employing the IEEE 802.1 x. protocol in said access point, if said user terminal utilizes the IEEE 802.1x. protocol; and,

means for employing an authentication means compatible with the user terminal if the user terminal employs a protocol other than the IEEE 802.1x protocol.

11. The access point in claim 10, wherein the means to determine includes means for communicating to the user terminal a Request-Identity extensible authentication protocol packet and if the user terminal utilizes the IEEE 802.1x protocol the access point receives a Response-Identity extensible authentication protocol packet.

12. The access point in claim 11, further comprises means to configure an internet protocol packet filtering means to redirect the user terminal request to a local server if the user terminal does not utilize said IEEE 802.1x protocol.

13. The access point in claim 10, further comprises means to communicate IEEE 802.1x protocol exchanges and means to establish internet protocol packet filtering through an internet protocol packet filter means and state information to control the user terminal access during and after an IEEE 802.1x based authentication process if the access point detects that the user terminal is IEEE 802.1x protocol compliant.

14. A method for controlling access by a user terminal in a wireless local area network by determining whether the user terminal utilizes an IEEE 802.1x protocol comprising the steps of:

an access point communicating to the user terminal a request to identify, and if the user terminal utilizes an IEEE 802.1x protocol, acknowledging the request to identify, otherwise the access point determining that the user terminal is not IEEE 802.1x compliant and selecting an authentication mechanism compatible with the user terminal.

15. The method according to claim 14, wherein the access point

determines that the user terminal is not IEEE 802.1x compliant when it does not receive an extensible authentication protocol identity response packet after a timeout value.

16. The method according to claim 15, further comprising the step of the access point detecting that if the user terminal is not IEEE 802.1x compliant, then configuring an internet protocol packet filter and redirecting a user request to a local server.

17. The method according to claim 16, further comprising the step of the local server communicating to the user terminal information specifically related to a browser based authentication protocol.

18. The method according to claim 17, further comprising the step of the access point transitioning to a state, if the user terminal utilizes the IEEE 802.1x protocol, that indicates that the user terminal is IEEE 802.1x compliant and thereafter processing all communication utilizing the IEEE 802.1x protocol.

19. The method according to claim 17, further comprising the step of the access point transitioning to a state corresponding to browser based authentication protocol if authentication fails.

20. The method according to claim 14, further comprising the step of the access point transitioning to a state corresponding to browser based authentication protocol if the user terminal is not IEEE 802.1x compliant.

21. A method for controlling access of a user terminal in a wireless local area network by determining whether the user terminal utilizes an IEEE 802.1x protocol, comprising the steps of:

communicating through an access point to the user terminal a request to identify, and if the user terminal utilizes an IEEE 802.1x protocol, acknowledging the request to identify, otherwise determining by the access point that the user terminal is not IEEE 802.1x compliant and selecting an authentication mechanism

compatible with the user terminal.

22. The method according to claim 21, further comprising the step of determining in the access point that the user terminal is not IEEE 802.1x compliant if the user terminal does not receive an extensible authentication protocol identity response packet after a preset time.

23. The method according to claim 21, further comprising the step of detecting in the access point if the user terminal is not IEEE 802.1x compliant, then configuring an internet protocol packet filter means and redirecting a user request to a local server.

24. The method according to claim 23, further comprising the step of communicating from the local server to the user terminal, information specifically related to a browser based authentication protocol.

25. The method according to claim 21, further comprising the step of transitioning to a state, in the access point if the user terminal utilizes the IEEE 802.1x protocol, that indicates that the user terminal is IEEE 802.1x compliant and thereafter processing all communication utilizing the IEEE 802.1x protocol.

26. The method according to claim 25, further comprising the step of transitioning to the state in the access point corresponding to browser based authentication protocol if authentication fails.

27. The method according to claim 21, further comprising the step of transitioning to a state in the access point corresponding to browser based authentication protocol if the user terminal is not IEEE 802.1x compliant.

Evidence Appendix

None

Related Proceedings Appendix

None